Scientific Research Publishing

Journal of Software Engineering and Applications, 2024, 17, 270-296
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

ERAD: Enhanced Ransomware Attack Defense System for Healthcare Organizations

Xinyue Li, Vijay K. Madisetti

School of Cybersecurity and Privacy, Georgia Institute of Technology, Atlanta, Georgia, USA
Email: xli3068@gatech.edu, vkm@gatech.edu

How to cite this paper: Li, X.Y. and Madisetti, V.K. (2024) ERAD: Enhanced Ransomware Attack Defense System for Healthcare Organizations. *Journal of Software Engineering and Applications*, **17**, 270-296.
https://doi.org/10.4236/jsea.2024.175016

Received: April 23, 2024
Accepted: May 25, 2024
Published: May 28, 2024

Abstract

Digital integration within healthcare systems exacerbates their vulnerability to sophisticated ransomware threats, leading to severe operational disruptions and data breaches. Current defenses are typically categorized into active and passive measures that struggle to achieve comprehensive threat mitigation and often lack real-time response effectiveness. This paper presents an innovative ransomware defense system, ERAD, designed for healthcare environments that apply the MITRE ATT&CK Matrix to coordinate dynamic, stage-specific countermeasures throughout the ransomware attack lifecycle. By systematically identifying and addressing threats based on indicators of compromise (IOCs), the proposed system proactively disrupts the attack chain before serious damage occurs. Validation is provided through a detailed analysis of a system deployment against LockBit 3.0 ransomware, illustrating significant enhancements in mitigating the impact of the attack, reducing the cost of recovery, and strengthening the cybersecurity framework of healthcare organizations, but also applicable to other non-health sectors of the business world.

Keywords

Ransomware, Healthcare Cybersecurity, MITRE ATT&CK Matrix, Incident Response, Ransomware Attack Lifecycle, Digital Health Safety

1. Introduction

In the digital era, healthcare's growing reliance on technology has significantly increased its vulnerability to cyberattacks, especially ransomware. This type of malware, which encrypts files or blocks access to computer systems until a ransom is paid, has surged in complexity and frequency [1]. Such attacks not only disrupt critical healthcare operations but also compromise sensitive patient data,

resulting in substantial financial and reputational damage.

From 2016 to 2021, the incidence of ransomware attacks on U.S. healthcare delivery organizations nearly doubled, escalating from 43 to 91 annual incidents [2]. In 2023, the healthcare sector continues to experience a surge in ransomware attacks, with 60% of organizations reporting such incidents, almost double the 34% in 2021 [3]. Dominant among these threats are Locker Ransomware and Crypto Ransomware [4]; the former locks users out of their systems without data compromise, while the latter encrypts critical files, demanding ransom for their release. A concerning trend is the rise of the "double dip" tactic, where data is not just encrypted but also exfiltrated, amplifying the potential for monetization [3]. This trend is further facilitated by the maturation of the ransomware-as-a-service (RaaS) model, which lowers the entry barriers and democratizes the means to launch attacks by providing low-cost, easily accessible ransomware tools online [1]. This model enables even individuals with minimal technical expertise to launch attacks, underscoring an urgent need for fortified defenses within healthcare institutions.

The impacts of ransomware in the healthcare sector are far-reaching, affecting financial stability, operational efficiency, reputational standing, and compliance with data privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) [5]. Financially, recovery costs have surged to an average of approximately $2.2 million per incident [3]. Operationally, nearly 45% of healthcare providers experience significant service disruptions, including prolonged downtimes and cancellations of scheduled care, which directly impact patient treatment [2]. The resulting reputational damage and concerns about data privacy can erode patient trust and have a long-term impact on healthcare organizations [1].

The importance of cybersecurity in healthcare is underscored by the high value of Protected Health Information (PHI), which includes sensitive data such as social security numbers, demographic details, and comprehensive medical records. It can be leveraged for identity theft, illegal drug purchases, or insurance fraud, making robust protection measures essential [6] [7]. Additionally, the healthcare industry faces unique challenges in safeguarding its IT infrastructure, including medical devices that can easily become cyber threat entry points [6] [8].

Traditional security measures in healthcare typically fall into proactive or reactive strategies, each with significant limitations. Proactive strategies, including employee awareness training and data backups, often fail due to the dynamic nature of cyber threats. Conversely, reactive strategies focus on mitigating damage after an incident occurs but are hindered by response delays and irreversible damage caused by attacks.

This paper introduces a *novel*, *stage-level* ransomware defense system, ERAD, that significantly enhances the cybersecurity defenses of healthcare organizations. Utilizing the MITRE ATT&CK Matrix [9], this system offers dynamic,

tailored responses to ransomware threats at each functional stage of their lifecycle. By providing sophisticated analysis and stage-specific countermeasures, the system not only prevents ransomware at its current stage but also anticipates and prepares for likely subsequent threats.

The proposed system's unique structure addresses the limitations of current defenses by integrating both proactive and responsive strategies to minimize attack impacts and facilitate rapid recovery. This paper will demonstrate the system's effectiveness through a detailed case study of the LockBit 3.0 ransomware [10], illustrating its strengths over traditional approaches and its adaptability to the evolving nature of cyber threats in healthcare.

The remainder of this paper is organized as follows: Section 2 discusses existing security approaches towards the ransomware issue and their limitations. Section 3 outlines the proposed solution and its key improvements. Section 4 describes the implementation details in the context of a case study on LockBit 3.0. Section 5 compares different approaches. Finally, Section 6 presents the conclusion.

2. Existing Work

Existing security measures against ransomware in healthcare are inherently categorized into two main strategies: proactive and reactive. Each strategy, while embodying the best practices in defense, reveals significant vulnerabilities that frequently leave healthcare organizations at risk. This section explores the primary security practices within these two categories and identifies the critical gaps between them, which the proposed system aims to address.

2.1. Proactive Approaches

Proactive strategies are designed to prevent ransomware from penetrating the organization. Primary methods include phishing awareness training and data backups, as recommended by the Health Sector Cybersecurity Coordination Center (HC3) [11]:

- Awareness Training: This training aims to educate healthcare personnel about cybersecurity threats and prevention techniques, such as recognizing phishing attempts, managing secure passwords, and safeguarding patient information. Despite its importance, current cybersecurity training often lacks a systematic approach and struggles to meet the rapidly evolving demands of digital healthcare environments. Clinicians report that due to high stress, time constraints, and workload pressures, medical personnel may not prioritize cybersecurity practices adequately [12], potentially leading to significant security gaps in handling sensitive patient information.
- Backup Systems: Essential for restoring systems and data after a ransomware attack, data backups themselves have increasingly become targets. Recent statistics indicate that 94% of organizations affected by ransomware have experienced attempts to compromise their backup systems during attacks [13].

This targeting undermines the reliability of backups as a robust fail-safe measure, exposing a significant vulnerability in proactive strategies.

- Attack Vector Restriction: Ransomware attackers utilize diverse tactics, rendering proactive measures like training and backups insufficient unless operations are significantly restricted [14]. In healthcare, where continuous service availability is critical, such restrictions are impractical and often inhibit proactive strategies from effectively countering various evolving attack methods.

2.2. Reactive Approaches

Reactive approaches are typically activated only after an incident occurs, focusing on damage control and system recovery:

- Sample Analysis: Research efforts have been directed at characterizing ransomware activity by analyzing collected samples from Windows [15] and mobile [16] systems to facilitate the identification of similar threats. However, the reactive nature of this approach means responses only occur after the ransomware has executed its payload, resulting in irreversible damage to files and systems [17]. Files encrypted before ransomware detection often remain irrecoverable, significantly disrupting patient care and hospital operations.
- Decryption Tools: Law enforcement and cybersecurity vendors have collaborated to produce decryption tools for specific ransomware variants, such as Coinvault [18] and LockBit [19]. Despite these efforts, the effectiveness of these tools is limited, and struggles to keep pace with the rapid evolution of ransomware tactics, underscoring the non-scalability of reactive solutions.
- Incident Response Plans: Many healthcare organizations lack a comprehensive incident response plan, critical for efficient recovery and minimizing service disruption. According to the Ponemon Institute [20], 40% of healthcare organizations lack a business continuity plan that accounts for system disruptions caused by ransomware. This absence can worsen the impact of an attack, extend recovery time, and increase overall costs.

2.3. Bridging the Gap: The Ransomware Attack Progression

Existing efforts seldom focus on the interval between the ransomware's entry into the organization and the commencement of data encryption. This critical period involves multiple functional stages of a ransomware attack, which, if addressed properly, could halt the attack's progression. The MITRE ATT&CK Matrix [9] serves as a pivotal tool in this context, which is a comprehensive knowledge base used for cyberattack modeling and simulation, providing a detailed understanding of adversary tactics and techniques based on real-world observations. This framework facilitates the visualization of an attacker's journey and the development of specific defenses against various stages of an attack, greatly enhancing cybersecurity across industries.

Utilizing the MITRE ATT&CK Matrix, this paper proposes a novel stage-level

ransomware defense system that effectively bridges the gaps between proactive and reactive approaches. The subsequent section details this system, highlighting how it combines the strengths of both strategic approaches to enhance healthcare organizations' ability to defend against ransomware.

3. ERAD: Our Proposed Approach

This paper introduces a ransomware attack defense system (ERAD) that equips hospitals with stage-level guidance for ransomware defense. Figure 1 depicts the high-level system workflow diagram, highlighting the system's focus on the intermediate period between ransomware entry into the organization and the encryption of services. The system categorizes the ransomware attack into various functional stages, such as initial access, data exfiltration to the Command and Control (C2) server, and impact on data and services. For each stage, the system conducts a thorough analysis based on detected indicators of compromise (IOCs), initially identifying the current stage of the ongoing ransomware attack. Subsequently, it delivers three types of crucial information to aid in ransomware defense:

1) Suggested preventive actions to halt the ransomware at its current stage.

2) Potential subsequent stages to which the ransomware could advance.

3) IOCs to monitor to verify the progression of the ransomware.

As illustrated in the ERAD system lifecycle flowchart (Figure 2), by analyzing ransomware activity and engaging actively with each stage of the ransomware attack lifecycle, the system can prevent the attack from reaching its most destructive phase, Impact. This preemptive approach minimizes the need for later-stage mitigation actions and reactive responses post-incident.

The system addresses the shortcomings of existing ransomware defense mechanisms by implementing stage-specific countermeasures. The key improvements include:

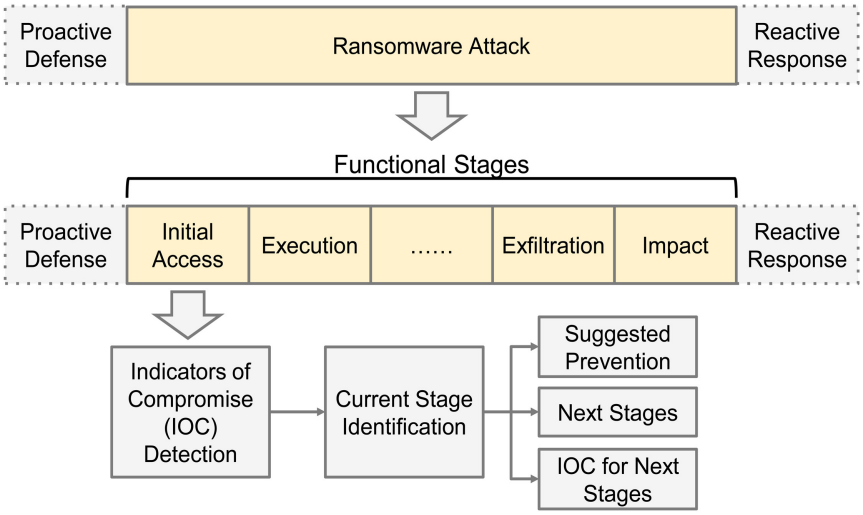

Figure 1. High-level workflow diagram of ERAD.

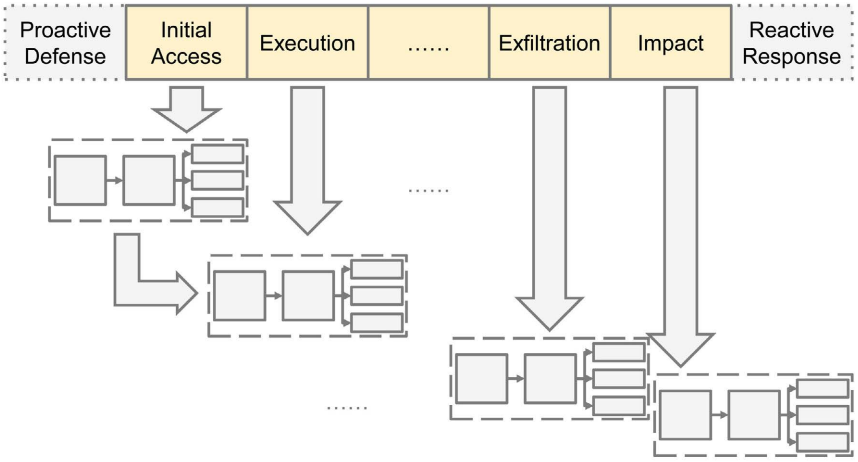

Figure 2. ERAD System lifecycle flowchart.

- Strategic Preventive Actions: The system not only predicts potential next stages but also prescribes suggested preventive actions for each stage, thereby maximizing the efficiency of interventions. This approach surpasses the reactive approach that involves high recovery costs and long downtimes, which are particularly severe for healthcare operations.
- Attack Lifecycle Engagement: By focusing on the full ransomware attack lifecycle, the system transitions from a binary defensive posture to a more nuanced, dynamic, stage-level response model. It empowers healthcare institutions to deploy strategic defenses that adapt to the ongoing attack, thus mitigating the limitations of both proactive and reactive approaches.
- Operational Impact Reduction: The system employs the Principle of Left of Boom, a concept borrowed from the healthcare and cybersecurity sectors, which focuses on preemptive actions to prevent critical incidents. This early intervention reduces the likelihood of extensive disruptions in healthcare services and accelerates a quicker return to normal operations. Therefore, the proposed solution successfully addresses the key challenge of long-term service disruptions in current defense approaches.
- Cost-effective Countermeasures: By anticipating and intercepting ransomware attacks during their development, the system mitigates potential financial and reputational damages, decreases the need for recovery procedures, and ensures a timely and cost-effective response ahead of catastrophic outcomes.

This advanced framework provides notable enhancements to the limitations of existing approaches, creates a more resilient defense architecture, and significantly enhances the security posture of healthcare organizations against ransomware threats.

4. Implementation and Test of ERAD

4.1. System Architecture

The architecture of the proposed ERAD system is shown in Figure 3, where the

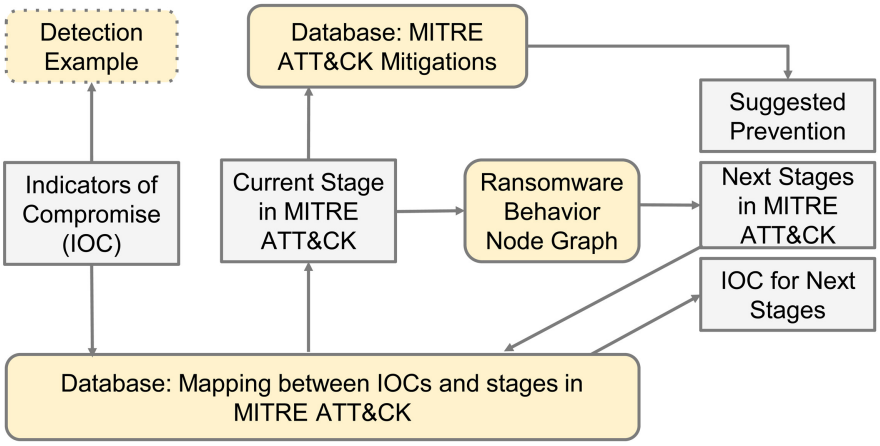

Figure 3. ERAD System architecture diagram.

components and their interconnections are depicted. The system inputs and outputs are represented by gray blocks and the implemented functional modules are represented by yellow blocks.

Initially, the system receives detected IOCs as input, which it immediately references against a database. This database contains the mapping relationships between IOCs and stages in the MITRE ATT&CK Matrix, pinpointing the current phase of the ongoing ransomware attack. Once the current stage is identified, the system proposes specific preventative actions by querying a separate database containing a comprehensive list of the MITRE ATT&CK's mitigations, crafting a defense tailored to the current threat level. Moving on, the system forecasts potential future stages in the MITRE ATT&CK Matrix where the ransomware might be proceeding next. The prediction is performed based on a ransomware behavior node graph, which underscores possible progression paths of the attack. In its final analytical phase, the system circles back to the mapping database to aggregate IOCs corresponding to each anticipated next stage, equipping the defense mechanism with threat intelligence to monitor the ransomware progression.

The introduction of the MITRE ATT&CK Matrix is particularly beneficial because it provides a structured, comprehensive framework for understanding and responding to ransomware tactics and techniques [9]. The framework facilitates a systematic approach to threat detection and response, enabling the system to provide precise, actionable insights. This dynamic functionality maintains a robust defense posture throughout the stages of a ransomware attack, significantly enhancing the overall security framework of the targeted healthcare organization.

4.2. Case Study Target

The implementation of the proposed system is based on a real-world scenario, using LockBit 3.0 as a case study. This ransomware variant was chosen because it was one of the top ransomware groups witnessed targeting the Healthcare and

Public Health Sector, as reported by HC3 [11].

LockBit 3.0 distinguishes itself not only through its prevalence but also through its adoption of advanced techniques that amplify its threat capability. The sophistication of LockBit 3.0 is reflected in its RaaS model, which broadens the scope of potential attackers by lowering entry barriers and extends the reach of ransomware [10]. The model is further enhanced by triple extortion schemes that combine traditional ransom demands with data disclosure threats and other extortion methods such as distributed denial-of-service (DDoS) attacks or direct threats to stakeholders [21] [22]. Additionally, LockBit 3.0's anti-analytics feature poses a significant challenge to cybersecurity defenses. By requiring a unique 32-character password for each boot, the ransomware effectively blocks many standard analytics techniques, calling for more advanced defense mechanisms [21].

To fight against the threats posed by LockBit 3.0, the system integrates critical threat intelligence from a Cybersecurity Advisory (CSA) [10] issued jointly by the FBI, CISA, and MS-ISAC. This advisory provides a rich dataset of recently and historically observed IOCs and analyzes tactics, techniques, and procedures (TTPs) based on the MITRE ATT&CK Matrix for Enterprise v13.1 [23]. The integration of this data enables the system to offer dynamic, responsive defenses tailored to threats posed by LockBit 3.0.

Through this real-world application, the system's potential to improve a hospital's security framework against advanced ransomware attacks will be validated, demonstrating the practical benefits of the proposed solution. The following subsections will explore the specific methodologies employed in the system's implementation and the results observed during the case study.

4.3. IOC-Stage Mapping Implementation and Detection Techniques

To enable the ERAD analysis system to identify the current stage of a ransomware attack, a database has been constructed that maps IOCs to stages in the MITRE ATT&CK Matrix. The types of IOCs included in this database are as follows [10] [24]:

- Registry Key: Changes to registry keys that are often manipulated to achieve persistence or escalate privileges.
- Freeware and Open-Source Tools: Legal software that LockBit 3.0 repurposes for malicious activities.
- Command Line Parameters: Specific commands used by the ransomware to automate encryption, spread across networks, or modify system configurations.
- IP Address and Domain Name: Network indicators related to LockBit 3.0's communication with C2 servers or sites utilized for data exfiltration.
- Service and Process Killed: Targeted termination of key operational or defensive services and processes to hinder response actions and maintain ransomware effectiveness.

The mapping results are illustrated in **Appendix A** Table A1. When the system receives an IOC as input, it consults this mapping database to determine the current stage of the attack. Once the potential next stages the ransomware may transition to are identified, the database is queried again to compile IOCs for each predicted stage. This provides precise guidance for ongoing monitoring and responsive actions.

Furthermore, the system incorporates detection examples for IOCs at each stage, as detailed in **Appendix A** Table A2. These detection methods are derived from cutting-edge ransomware detection techniques that focus on early-stage identification. They validate the feasibility of this system and provide insights into detecting ransomware at various stages.

4.4. Preventive Action Database Implementation

Once the current stage of a ransomware attack within the MITRE ATT&CK Matrix is determined, the system proposes specific preventive actions to halt the attack. To ensure consistency and granularity, a database organizing mitigations from the MITRE ATT&CK Matrix has been developed, as shown in **Appendix A** Table A3. The preventive actions are categorized into two types: immediate containment actions and broader general mitigation actions.

1) Containment actions are designed to prevent the ransomware from spreading further. These include taking offline the affected resources, isolating them from the network, and removing vulnerable software or devices. They correspond to Network Segmentation (M1030) and Disable or Remove Feature or Program (M1042) in MITRE ATT&CK Matrix.

2) General mitigation actions, on the other hand, go beyond immediate containment to address specific techniques used at the current stage of the attack. These actions are tailored to reflect the threat tactics employed by the attacking ransomware, enhancing the precision of defense strategies.

For instance, if LockBit 3.0 is identified at the Initial Access stage, the database reveals that one of its common techniques at this stage is External Remote Services (T1133). Accordingly, the system recommends containment actions such as Network Segmentation (M1030) and Disable or Remove Feature or Program (M1042) to block remote access and deactivate related services. Additionally, general mitigations like Limit Access to Resource Over Network (M1035) and Multi-factor Authentication (M1032) are suggested to control network access and strengthen authentication protocols. This approach not only disrupts the ransomware's progression but also adapts the defense mechanisms to be as dynamic and specific as the threats.

4.5. Behavioral Node Graph Construction

To help hospitals track the progression of ransomware attacks, the proposed system forecasts potential movements of ransomware through a behavioral node graph. Although the MITRE ATT&CK Matrix effectively categorizes an attack

into distinct stages and suggests a typical progression path, it does not fully consider the non-sequential behavior of ransomware that often jumps back and forth between stages. For example, if LockBit 3.0 reaches the Privilege Escalation stage, it might choose to evade defenses, as outlined in the linear matrix (Defense Evasion stage), or it may attempt to solidify its presence (Persistence), which is an earlier stage.

To address this limitation, the ERAD system utilizes a behavioral node graph (**Figure 4**) to map the possible paths of ransomware. The graph visually represents each stage as a node linking to a potential subsequent stage, providing a more detailed understanding of the ransomware path. The node graph begins with the Initial Access stage on the left and guides defenders in preventing the ransomware from reaching the final Impact stage on the right, where significant data damage may occur.

The construction of this node graph is based on a detailed behavioral analysis of LockBit 3.0, leveraging insights from CSA's analysis of ATT&CK techniques. As an example, in the Privilege Escalation stage, LockBit 3.0 may employ the Domain Policy Modification: Group Policy Modification (T1481.001) technique, preparing it for lateral movements, thereby suggesting Lateral Movement as a likely subsequent stage of Privilege Escalation.

The implementation of the behavioral node graph significantly improves the linear MITRE ATT&CK Matrix by providing a multi-dimensional view of ransomware progression, better reflecting the complex behavior of threats such as LockBit 3.0. This enhancement enables defenders to visualize a wider range of attack scenarios and adapt more quickly to changing techniques. By improving the accuracy of ransomware movement predictions, behavioral node graphs help strategically deploy countermeasures, transforming the traditional Matrix into a dynamic and customizable tool to enhance ransomware defenses against the

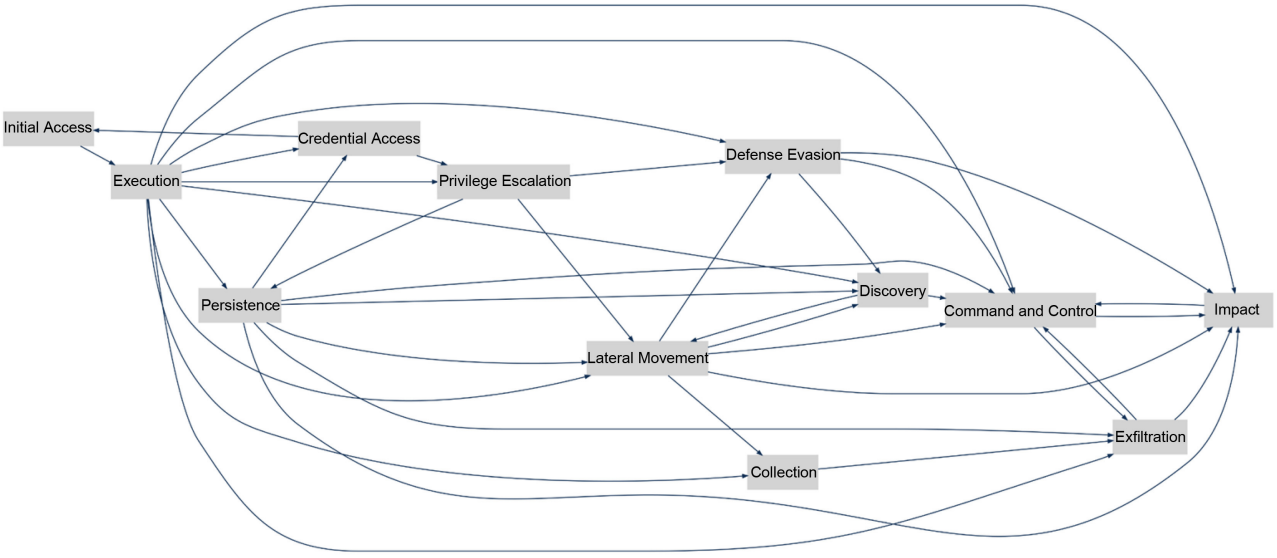

Figure 4. Behavioral node graph (visualized with Python NetworkX library) presented in ERAD.

complexity of modern ransomware threats.

4.6. System Interface Design and Functional Demonstration

Figure 5 showcases a preliminary Graphic User Interface (GUI) prototype developed using the Python tkinter library. This GUI is designed for demonstration purposes and to exhibit the main functionalities of the proposed system. The screenshot illustrates a particular use case.

When the remote desktop software Splashtop is detected, it is entered into the system as an IOC. Given that LockBit 3.0 frequently utilizes this software to enable lateral movement, the system determines that the attack has reached the Lateral Movement stage. Building on this identification, the system consults the behavioral node graph to discover possible future stages to which the ransomware may progress. It then offers suggested mitigations to stop LockBit 3.0 at the current stage and outlines IOCs for each potential future stage. This enables defenders to continuously monitor the ransomware's progress.

The interface is designed to streamline complex data interactions, rendering the analysis and decision-making processes more intuitive and accessible for security personnel. This facilitation significantly enhances the system's usability in fast-paced security environments.

5. Comparison with Prior Work

This section contrasts the effectiveness of the proposed stage-level ransomware

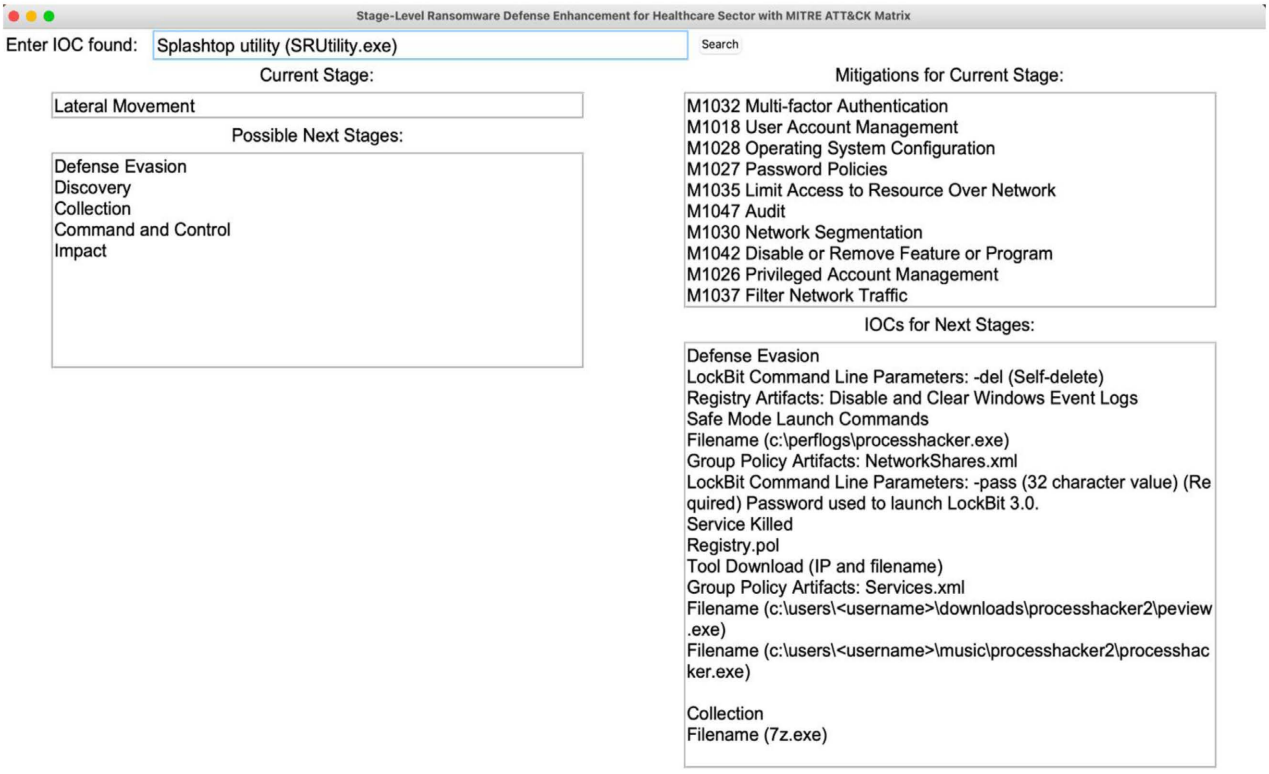

Figure 5. ERAD GUI and system demonstration.

defense system, ERAD, with traditional proactive and reactive strategies, highlighting its advancements in mitigating operational impacts on healthcare facilities. While proactive and reactive approaches have their merits, they fall short in the critical context of healthcare operations. In healthcare settings, maintaining a high operational level is not only a matter of efficiency but a key to patient care and safety. Any disruption can result in immediate and severe consequences for patient health, making the continuity of operations a top priority. The following graphical analysis (Figure 6) reflects how the operational level is impacted during a ransomware attack under different approaches.

The blue line in both charts symbolizes the proposed approach, initiating a response at the first sign of ransomware entry. This immediate action results in a temporary operational decline as the system mitigates the threat, allowing the organization to continue at a reduced capacity during recovery.

In the "Proposed & Proactive Approaches" chart, the green line representing the proactive strategy shows frequent and significant operational interruptions. This demonstrates the aggressive nature of the proactive approach, which often

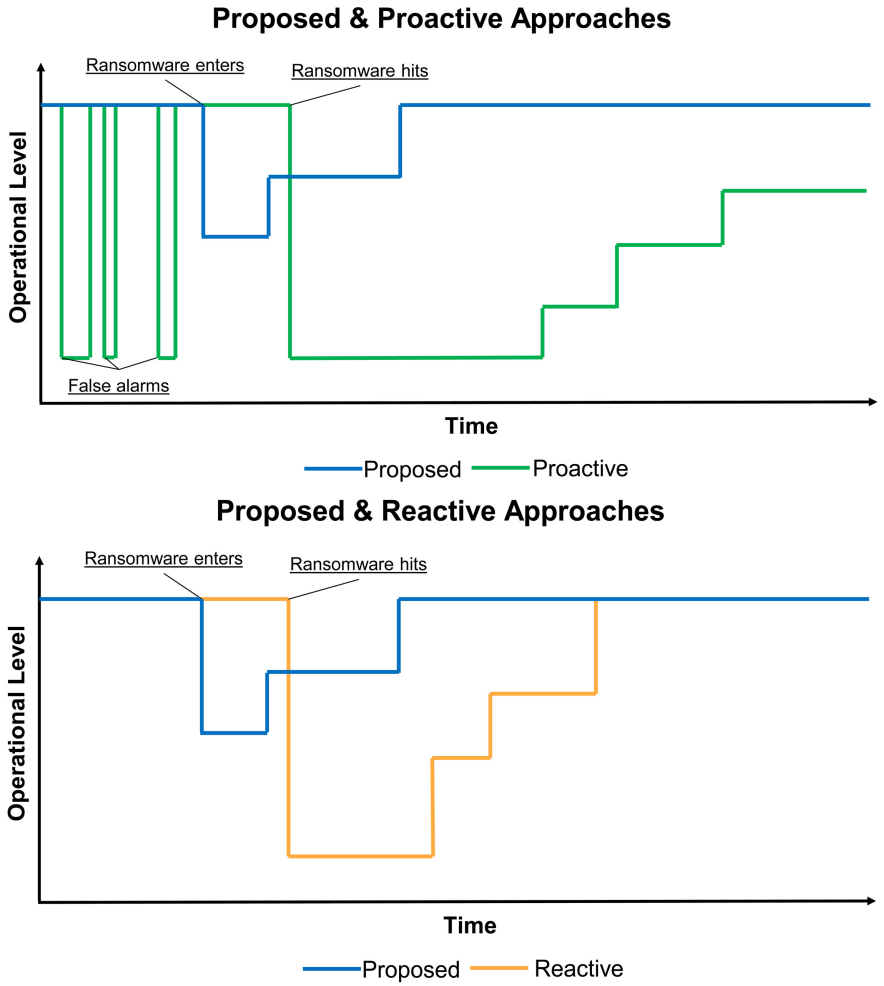

Figure 6. Comparative analysis of proposed, proactive, and reactive ransomware defense approaches over time.

preemptively halts operations to prevent ransomware infiltration. This can block some threats, but it also introduces too many false alarms and operational stops, leading to instability and inefficiency. Moreover, when a proactive system is eventually broken by a sophisticated attack, it experiences longer recovery times.

In the "Proposed & Reactive Approaches" chart, the orange line illustrates the reactive approach, which maintains normal operations until an attack occurs and then focuses on quick incident response. However, this strategy leads to a significant drop in the level of operation followed by a long recovery time once data and infrastructure are affected by an attack.

Through this analysis, the proposed ERAD system demonstrates its ability to maintain higher operational continuity and stability over time, unlike the fluctuations and severe declines seen with traditional proactive and reactive methods. By focusing on early detection and response, the proposed system reduces both the time and the resources required for post-attack recovery.

A case study of the LockBit 3.0 attack on Carthage Area Hospital [25] and Claxton-Hepburn Medical Center [26] serves to further illustrate the effectiveness:

Incident Introduction:

In late August of 2023, LockBit 3.0 attacked Carthage Area Hospital and Claxton-Hepburn Medical Center, critical healthcare institutions serving a combined populace of over 200,000 in upstate New York.

Timeline of the Attack [27] [28]:

- August 31, 2023: a ransomware infiltration occurred that severely disrupted hospital operations. The attack resulted in immediate outpatient appointments being rescheduled and the diversion of emergency room services to other facilities, which significantly impacted healthcare delivery.
- September 2, 2023: The phone system was quickly restored, yet the rescheduling of appointments continues, indicating ongoing disruption.
- September 6, 2023: Investigations revealed that sensitive personal and health information including names, addresses, birth dates, and social security numbers had been compromised, raising serious privacy and security concerns.
- September 15, 2023: The LockBit ransomware organization publicly claimed responsibility for the attack.
- September 19, 2023: A deadline was set by the attackers for the ransom payment, with the threat that failure to comply would result in the publication of the stolen data.

Impact Analysis:

The full details of this attack remain under investigation, with critical information regarding the breach's techniques and the exact financial impact still undisclosed. As a result, the impact analysis will be qualitative, focusing on the broader implications and disruptions such incidents can cause within healthcare systems.

The immediate effects included a healthcare service disruption that spanned over two weeks, emergency room closure due to compromised operational capacities, and outpatient appointments postponed or canceled. This disruption strained nearby medical facilities as patients were diverted. The hospitals' digital infrastructure, which is the lifeline of modern healthcare services, was also greatly impacted. Key IT assets such as the internal phone systems were made unavailable, blocking communication channels within the hospitals. Digital systems such as Electronic Health Record (EHR) system, hospital digital medication system, and digital laboratory system were affected, resulting in potential delays in diagnosis and treatment. From a financial perspective, while specific figures regarding the costs incurred by this incident or the demanded ransom amount remain undisclosed, statistics show that the average recovery cost for similar breaches in healthcare organizations is approximately $2.2 million [3]. This figure provides a reference for the potential economic burden that the affected hospitals may face. The attack also had compliance and reputational impacts that were more diffuse and challenging to quantify but arguably just as impactful. Compliance violations, such as potential breaches of HIPAA due to compromised patient health information, can lead to fines, further limiting the hospitals' resources. Moreover, the reputational damage caused by such attacks could erode patient trust, which is critical to the healthcare industry, and could influence patient decisions long after the incident is resolved.

Reduced Impact with Proposed System:

The proposed system empowers hospitals to substantially mitigate the operational and financial impacts of ransomware attacks. By detecting ransomware activity before it progresses to the stages of data exfiltration or encryption, the system can significantly minimize service disruptions. Consequently, rescheduled outpatient appointments, emergency room diversions, and closures might be entirely avoided, maintaining the continuity of critical health care services. From an IT perspective, the system's early detection capability enables organizations to quickly isolate affected devices, effectively limiting the impact and keeping critical services available. Financially, the avoidance of widespread system encryption would likely lead to a decrease in recovery costs and ransom demands. While reputational damage and HIPAA compliance risks depend on the extent of data involved, the system's rapid response is expected to mitigate the severity of any breach, thereby limiting the scope of reputational damage and potential compliance violations.

6. Summary and Conclusions

This paper proposes a novel stage-level ransomware defense system, ERAD, that leverages the MITRE ATT&CK Matrix to deliver dynamic, stage-specific responses tailored to the unique challenges of the healthcare sector. By responding to IOCs and implementing strategic preventive actions, the system can effectively prevent ransomware attacks from reaching their most damaging stages, the-

reby safeguarding critical healthcare operations and sensitive patient data. The paper further illustrated the real-world applicability of this system through a case study on the LockBit 3.0 ransomware.

Future Directions: To enhance the system's effectiveness, incorporating comprehensive impact analyses at each stage of an attack could significantly refine decision-making processes, enabling healthcare organizations to better tailor preventive and mitigative strategies. Additionally, extending the system's coverage to include mobile and Internet of Things (IoT) devices is essential, as these technologies are becoming increasingly prevalent in healthcare settings and introduce new security vulnerabilities. Integrating the MITRE ATT&CK Matrix for Mobile and Industrial Control Systems (ICS) could address these challenges comprehensively. Advancing these aspects will ensure the proposed ERAD can be developed further to protect critical healthcare infrastructure and sensitive patient information against increasingly sophisticated cyber threats.

Acknowledgements

We thank the reviewers for their detailed comments that greatly improved the paper.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Gagneja, K.K. (2017) Knowing the Ransomware and Building Defense against It—Specific to Healthcare Institutes. 2017 *Third International Conference on Mobile and Secure Services* (*MobiSecServ*), Miami Beach, 11-12 February 2017, 1-5. https://doi.org/10.1109/MOBISECSERV.2017.7886569

[2] Neprash, H.T., *et al.* (2022) Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, **3**, e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

[3] Mahendru, P. (2023) The State of Ransomware in Healthcare 2023. Sophos News. https://news.sophos.com/en-us/2023/08/10/the-state-of-ransomware-in-healthcare-2023/

[4] Thamer, N. and Alubady, R. (2021) A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. 2021 1*st Babylon International Conference on Information Technology and Science* (*BICITS*), Babil, 28-29 April 2021, 210-216. https://doi.org/10.1109/BICITS51482.2021.9509877

[5] Nikki, S., *et al.* (2018) Ransomware in Healthcare Facilities: A Harbinger of the Future? *Perspectives in Health Information Management*, **15**, 1-22. https://www.proquest.com/scholarly-journals/ransomware-healthcare-facilities-harbinger-future/docview/2111721098/se-2

[6] Bhosale, K.S., Nenova M. and Iliev, G. (2021) A Study of Cyber Attacks: In the Healthcare Sector. 2021 *Sixth Junior Conference on Lighting* (*Lighting*), Gabrovo, 23-25 September 2021, 1-6. https://doi.org/10.1109/Lighting49406.2021.9598947

[7] Mohamad Al-Aboosi, A.M., Huda Sheikh Abdullah, S.N., Murah, M.Z. and Al Dharhani, G.S. (2022) Cybersecurity Trends in Health Information Systems. 2022 *International Conference on Cyber Resilience* (*ICCR*), Dubai, 6-7 October 2022, 1-4. https://doi.org/10.1109/ICCR56254.2022.9995952

[8] Kelly, W.H., *et al*. (2023) Triumph Over Adversity: Unlocking Optimal Trauma Outcomes during Healthcare Ransomware Attacks. *Injury*, **54**, Article 111046. https://doi.org/10.1016/j.injury.2023.111046

[9] Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A. and Thomas, C. (2018) MITRE ATT&CK®: Design and Philosophy. https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf

[10] Joint Cybersecurity Advisory TLP Clear: Understanding Ransomware Threat Actors: Lockbit. AHA. https://www.aha.org/cybersecurity-government-intelligence-reports/2023-06-14-joint-cybersecurity-advisory-tlp-clear-understanding-ransomware-threat

[11] Office of Information Security and Health Sector Cybersecurity Coordination Center (2024) Ransomware & Healthcare. https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf

[12] Frati, F., Darau, G., Salamanos, N., *et al*. (2024) Cybersecurity Training and Healthcare: The AERAS Approach. *International Journal of Information Security*, **23**, 1527-1539. https://doi.org/10.1007/s10207-023-00802-y

[13] Adam, S. (2024) The Impact of Compromised Backups on Ransomware Outcomes. Sophos News. https://news.sophos.com/en-us/2024/03/26/the-impact-of-compromised-backups-on-ransomware-outcomes/

[14] Maigida, A.M., Abdulhamid, S.M., Olalere, M., Alhassan, J.K., Chiroma, H. and Dada, E.G. (2019) Systematic Literature Review and Metadata Analysis of Ransomware Attacks and Detection Mechanisms. *Journal of Reliable Intelligent Environments*, **5**, 67-89. https://doi.org/10.1007/s40860-019-00080-3

[15] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L. and Kirda, E. (2015) Cutting the Gordian Knot: A Look under the Hood of Ransomware Attacks. *Detection of Intrusions and Malware, and Vulnerability Assessment*, Milan, 9-10 July 2015, 3-24. https://doi.org/10.1007/978-3-319-20550-2_1

[16] Andronio, N., Zanero, S. and Maggi, F. (2015) HELDROID: Dissecting and Detecting Mobile Ransomware. *Research in Attacks, Intrusions, and Defenses*, Kyoto, 2-4 November 2015, 382-404. https://doi.org/10.1007/978-3-319-26362-5_18

[17] Kolodenker, E., Koch, W., Stringhini, G. and Egele, M. (2017) PayBreak: Defense against Cryptographic Ransomware. *Proceedings of the* 2017 *ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi, 2-6 April 2017, 599-611. https://doi.org/10.1145/3052973.3053035

[18] Pauli, D. (2015) Kaspersky Announces 'Death' of Coinvault, Bitcryptor Ransomware. https://www.theregister.com/2015/11/02/kaspersky_announces_death_of_coinvault_bitcryptor_ransomware/

[19] Office of Public Affairs (2024) U.S. and U.K. Disrupt LockBit Ransomware Variant. United States Department of Justice. https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant

[20] The Impact of Ransomware on Patient Safety and the Value of Cybersecurity Benchmarking. Censinet. https://www.censinet.com/

[21] Mckeon, J. (2022) HHS Warns Healthcare Sector of LockBit 3.0, BlackCat Ransomware. Health IT Security. https://healthitsecurity.com/news/hhs-warns-healthcare-sector-of-lockbit-3.0-blackcat-ransomware

[22] Triple Extortion Ransomware. Security. https://www.techtarget.com/searchsecurity/definition/triple-extortion-ransomware

[23] Matrix-Enterprise. MITRE ATT&CKTM. https://attack.mitre.org/ https://attack.mitre.org/matrices/enterprise/

[24] CISA (2023) #StopRansomware: LockBit 3.0. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

[25] Cyber Announcement-Carthage Area Hospital. https://www.carthagehospital.com/cyber-announcement/

[26] Cyber Announcement. Claxton-Hepburn Medical Center. https://www.claxtonhepburn.org/corporate-compliance/cyber-announcement/

[27] Greig, J. (2023) Upstate New York Nonprofit Hospitals Still Facing Issues after LockBit Ransomware Attack. https://therecord.media/upstate-new-york-hospitals-ransomware-attack

[28] Global Edition and Privacy & Security (2023) New York Community Hospitals Still Impacted by Lockbit Attack, Weeks Later. Healthcare IT News. https://www.healthcareitnews.com/news/new-york-community-hospitals-still-impacted-lockbit-attack-weeks-later

[29] Kok, S.H., Abdullah, A. and Jhanjhi, N. (2020) Early Detection of Crypto-Ransomware Using Pre-Encryption Detection Algorithm. *Journal of King Saud University-Computer and Information Sciences*, **34**, 1984-1999. https://doi.org/10.1016/j.jksuci.2020.06.012

[30] Khammas, B.M. (2020) Ransomware Detection Using Random Forest Technique. *ICT Express*, **6**, 325-331. https://doi.org/10.1016/j.icte.2020.11.001 .

[31] Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S. and Khayami, R. (2020) Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence. *IEEE Transactions on Emerging Topics in Computing*, **8**, 341-351. https://doi.org/10.1109/TETC.2017.2756908

[32] Mohaisen, A., Alrawi, O. and Mohaisen, M. (2015) AMAL: High-Fidelity, Behavior-Based Automated Malware Analysis and Classification. *Computers & Security*, **52**, 251-266. https://doi.org/10.1016/j.cose.2015.04.001

[33] Gangwar, K., Mohanty, S. and Mohapatra, A.K. (2018) Analysis and Detection of Ransomware through Its Delivery Methods. *Data Science and Analytics*, Gurgaon, 13-14 October 2017, 353-362. https://doi.org/10.1007/978-981-10-8527-7_29

[34] Roy, K.C. and Chen, Q. (2020) DeepRan: Attention-Based BiLSTM and CRF for Ransomware Early Detection and Classification. *Information Systems Frontiers*, **23**, 299-315. https://doi.org/10.1007/s10796-020-10017-4

[35] Cabaj, K., Gregorczyk, M. and Mazurczyk, W. (2018) Software-Defined Networking-Based Crypto Ransomware Detection Using HTTP Traffic Characteristics. *Computers & Electrical Engineering*, **66**, 353-368. https://doi.org/10.1016/j.compeleceng.2017.10.012

[36] Alhawi, O.M.K., Baldwin, J. and Dehghantanha, A. (2018) Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection. In: Dehghantanha, A., Conti, M. and Dargahi, T., Eds., *Cyber Threat Intelligence*,

Springer, Cham, 93-106. https://doi.org/10.1007/978-3-319-73951-9_5

[37] Intel® Threat Detection Technology: Better Protect Your PC Fleet from Advanced Cyberattacks. https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/hardware-shield/threat-detection-technology.html

[38] Mehnaz, S., Mudgerikar, A. and Bertino, E. (2018) RWGuard: A Real-Time Detection System against Cryptographic Ransomware. *Research in Attacks*, *Intrusions*, *and Defenses*, Heraklion, Crete, 10-12 September 2018, 114-136. https://doi.org/10.1007/978-3-030-00470-5_6

Appendix A: Tables

Table A1. Mapping between IOCs and stages.

IOC	Stage
Filename (7z.exe)	Collection
FTP to Russian geolocated IP from compromised system Network Connections (IP) User Agent Strings Command interpreter (Plink.exe) Anydesk Usage (IP) Remote admin tool (AnyDeskMSI.exe) Tools (Action1, Atera, anydesk, fixme it, screenconnect, splashtop, zoho assist) Domain (eu1-dms.zoho[.]eu, fixme[.]it, unattended.techninline[.]net)	Command and Control
Filename (c:\perflogs\lsass.dmp) Filename (c:\users\<username>\downloads\mimikatz.exe) Filename (c:\users\<username>\desktop\proc64\proc.exe)	Credential Access
Group Policy Artifacts: NetworkShares.xml Registry.pol Safe Mode Launch Commands Group Policy Artifacts: Services.xml Service Killed Filename (c:\users\<username>\downloads\processhacker2\peview.exe) Filename (c:\users\<username>\music\processhacker2\processhacker.exe) Filename (c:\perflogs\processhacker.exe) Registry Artifacts: Disable and Clear Windows Event Logs LockBit Command Line Parameters: -del (Self-delete) LockBit Command Line Parameters: -pass (32 character value) (Required) Password used to launch LockBit 3.0. Tool Download (IP and filename)	Defense Evasion
Network scanning software (Netscan.exe) Filename (tniwinagent.exe)	Discovery
PowerShell script (123.ps1) Force GPUpdate Filename (psexesvc.exe) Mutual Exclusion Object (Mutex) Created	Execution
Filename (c:\windows\temp\screenconnect\23.8.5.8707\files\azure.msi)	Exfiltration
Volume Shadow Copy Deletion	Impact

Continued

LockBit Command Line Parameters: -path (File or path) Only encrypts provided file or folder.	
Lockbit 3.0 Ransom Note	
LockBit 3.0 Black Icon (and also registry artifacts)	
LockBit 3.0 Wallpaper (and also registry artifacts)	
LockBit Command Line Parameters: -wall (Sets LockBit 3.0 Wallpaper and prints out LockBit 3.0 ransom note)	
Volume Shadow Copy Deletion	
Group Policy Artifacts: Services.xml	
Service Killed	
Processes Killed	
Suspicious Email Activity	Initial Access
LockBit Command Line Parameters: -gspd (Spread laterally via group policy) & -psex (Spread laterally via admin shares)	Lateral Movement
Splashtop utility (SRUtility.exe)	
LockBit Command Line Parameters: -safe (Reboot host into Safe Mode)	Persistence
Registry Artifacts: Enable Automatic Logon	
Ransom Locations	
Scheduled task: \MEGA\MEGAcmd	
Scheduled task: UpdateAdobeTask	
Mag.dll	
UAC Bypass Via Elevated COM Interface	Privilege Escalation
LockBit Command Line Parameters: -safe (Reboot host into Safe Mode)	
Registry Artifacts: Enable Automatic Logon	
LockBit Command Line Parameters: -gdel (Remove LockBit 3.0 group policy changes)	
Group Policy Artifacts: NetworkShares.xml	
Force GPUpdate	
Ransom Locations	

Table A2. Techniques and detection examples for each stage.

Stage	Techniques	Detection Example
Initial Access	Valid Accounts (T1078) Exploit External Remote Services (T1133) Drive-by Compromise (T1189) Exploit Public-Facing Application (T1190) Phishing (T1566)	Reference [29] on creating a ransomware signature database and developing a dataset for machine learning-based prediction provides critical tools for detecting early-stage ransomware attacks. By incorporating SHA-256 hash values of ransomware identifiers into the database, this work enables the identification of specific ransomware variants at this stage. Additionally, the machine learning model trained on this dataset can help predict and flag activities related to techniques like phishing or exploiting public-facing applications, which are commonly utilized by LockBit 3.0.
Execution	Command and Scripting Interpreter: Windows Command Shell (T1059.003) System Services: Service Execution (T1059.002)	Reference [30] focuses on using machine learning techniques to categorize ransomware, particularly through the implementation of a Random Forest classifier. By extracting features from the raw bytes of an executable file, the method is effective in identifying ransomware-related activities, such as those involving Windows Command Shell or service execution.
Persistence	Boot or Logo Autostart Execution (T1547) Valid Accounts (T1078)	Reference [31] leverages sequential pattern mining and machine learning techniques to effectively identify ransomware at the Persistence stage. By focusing on specific events like registry modifications, Dynamic Link Library (DLL) interactions, and scheduled tasks, the system can rapidly distinguish between benign applications and ransomware. Achieving a high F-measure and Area Under the Curve (AUC) value, this approach ensures accurate and early detection of ransomware behaviors such as those involving command line parameters and registry artifacts used by LockBit 3.0.
Privilege Escalation	Abuse Elevation Control Mechanism (T1548) Boot or Logo Autostart Execution (T1547) Domain Policy Modification: Group Policy Modification (T1484.001) Valid Accounts (T1078)	Reference [32] proposes AMAL, an automated malware analysis system. AMAL's AutoMal subsystem excels in collecting detailed behavioral artifacts from the file system, memory, network, and especially the registry, which are critical in identifying changes made by LockBit 3.0, particularly group policy modifications. By analyzing these artifacts, AMAL can effectively differentiate between normal system modifications and malicious alterations linked to ransomware tactics. Furthermore, MaLabel, the classification component of AMAL, leverages these detailed artifacts to accurately classify malware samples into families, aiding in the quick identification of LockBit 3.0 based on its unique behavior patterns observed during privilege escalation activities.
Defense Evasion	Domain Policy Modification: Group Policy Modification (T1484.001) Impair Defenses: Disable or Modify Tools (T1562.001) Indicator Removal: Clear Windows Event Logs (T1070.001) Indicator Removal: File Deletion (T1070.004) Obfuscated Files or Information (T1027)	Reference [33] introduces a method for detecting ransomware attacks at early stages by analyzing behavioral patterns, such as file paths, dropped files, and network activities, which are critical in identifying defense evasion techniques used by LockBit 3.0. By employing machine learning algorithms, particularly the random forest classifier, this approach achieves high accuracy in classifying ransomware based on extracted features, including those related to Group Policy modifications and obfuscation methods observed.

Continued

Credential Access	OS Credential Dumping: LSASS Memory (T1003.001) Brute Force (T1110)	The research on the Pre-Encryption Detection Algorithm (PEDA) [29] which utilizes SHA-256 hashing to compare potential malicious files against a comprehensive database of ransomware signatures, effectively identifying known ransomware-related files such as lsass.dmp and mimikatz.exe before the ransomware is activated.
Discovery	Network Service Discovery (T1046) System Information Discovery (T1082) System Location Discovery: System Language Discovery (T1614.001)	Further applying the PEDA [29] previously utilized in the Credential Access stage, this approach extends its detection capabilities into the Discovery stage. By employing SHA-256 hashing, PEDA effectively compares incoming file signatures against a database of known ransomware identifiers. This enables the early identification of tools like Netscan.exe and tniwinagent.exe, which LockBit 3.0 employs for Network Service Discovery and System Information Discovery techniques.
Lateral Movement	Remote Services: Remote Desktop Protocol (T1021.001) Remote Services: Server Message Block (SMB)/Admin Windows Shares (T1021.002)	The DeepRan system [34] utilizes an innovative Term Frequency-Inverse Document Frequency (TF-IDF) approach combined with an attention-based BiLSTM network to detect anomalies in network behavior that indicate unauthorized Remote Desktop Protocol (RDP) or Server Message Block (SMB) activities, commonly exploited by LockBit 3.0 for spreading across the network. When LockBit employs techniques such as modifying group policies or using admin shares for lateral movements, DeepRan can identify these deviations by comparing them against typical host patterns, thus preventing the ransomware from infecting additional hosts within the network.
Collection	Archive Collected Data: Archive via Utility (T1560.001)	Continuing to leverage the PEDA [29] established in earlier stages, which can use SHA-256 hashing to swiftly identify and flag suspicious utilities like 7z.exe, which LockBit 3.0 may use for archiving collected data. By comparing the signatures of files associated with Archive via Utility techniques against its extensive ransomware signature database, PEDA helps prevent the unauthorized consolidation of sensitive information.
Command and Control	Application Layer Protocol: File Transfer Protocols (T1071.002) Application Layer Protocol: Web Protocols (T1071.001) Protocol Tunneling (T1572) Remote Access Software (T1219)	Reference [35] puts forward a SDN-based detection system that identifies ransomware communication by analyzing HTTP traffic patterns, focusing on message sequences and sizes. By inspecting outgoing HTTP POST data, it effectively detects connections between infected hosts and C2 servers.
Exfiltration	Exfiltration Over Web Service (T1567) Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)	Reference [36] introduces NetConverse, a machine learning-based system particularly effective in monitoring and analyzing network traffic associated with Windows ransomware. This system specializes in detecting anomalous data transfers that occur during the Exfiltration stage of a ransomware attack, such as those introduced by LockBit 3.0. By analyzing network conversations that emerge when ransomware attempts to exfiltrate data to cloud storage or other web services, NetConverse can identify suspicious activity with a high degree of accuracy.

Continued

Impact	Data Destruction (T1485) Data Encrypted for Impact (T1485) Defacement: Internal Defacement (T1491.001) Inhibit System Recovery (T1490) Service Stop (T1489)	The Threat Detection Technology [37] proposed by Intel mines low-level hardware telemetry directly from the CPU's Performance Monitoring Unit (PMU). It identifies the distinct operational fingerprint of malware execution such as encryption in real time with minimal disruption. The RWGuard system, as outlined in Reference [38], provides a robust method to combat ransomware during the Impact stage. This system utilizes a combination of decoy files, process monitoring, and file change monitoring to quickly detect and counter ransomware activities aimed at data destruction and encryption.

Table A3. Preventive action database.

Stage	Technique	Mitigation
Collection	Archive Collected Data: Archive via Utility	M1047 Audit
Command and Control	Application Layer Protocol: File Transfer Protocols	M1031 Network Intrusion Prevention
		M1030 Network Segmentation
	Non-Application Layer Protocol	M1031 Network Intrusion Prevention
		M1037 Filter Network Traffic
	Protocol Tunneling	M1031 Network Intrusion Prevention
		M1037 Filter Network Traffic
	Remote Access Software	M1031 Network Intrusion Prevention
		M1037 Filter Network Traffic
		M1038 Execution Prevention
Credential Access	Brute Force	M1018 User Account Management
		M1027 Password Policies
		M1032 Multi-factor Authentication
		M1036 Account Use Policies
	Credentials from Password Stores: Credentials from Web Browsers	M1027 Password Policies
	Credentials from Password Stores: Windows Credential Manager	M1042 Disable or Remove Feature or Program
	OS Credential Dumping: LSASS Memory	M1017 User Training
		M1025 Privileged Process Integrity
		M1026 Privileged Account Management
		M1027 Password Policies
		M1028 Operating System Configuration
		M1040 Behavior Prevention on Endpoint
		M1043 Credential Access Protection

Continued

Defense Evasion	Abuse Elevation Control Mechanism: Bypass User Account Control	M1026 Privileged Account Management
		M1047 Audit
		M1051 Update Software
		M1052 User Account Control
	Domain Policy Modification: Group Policy Modification	M1018 User Account Management
		M1026 Privileged Account Management
		M1047 Audit
	Execution Guardrails: Environmental Keying	M1055 Do Not Mitigate
	Impair Defenses: Disable or Modify Tools	M1018 User Account Management
		M1022 Restrict File and Directory Permissions
		M1024 Restrict Registry Permissions
		M1038 Execution Prevention
	Indicator Removal: Clear Windows Event Logs	M1022 Restrict File and Directory Permissions
		M1029 Remote Data Storage
		M1041 Encrypt Sensitive Information
	Obfuscated Files or Information: Software Packing	M1049 Antivirus/Antimalware
	Valid Accounts	M1013 Application Developer Guidance
		M1015 Active Directory Configuration
		M1017 User Training
		M1018 User Account Management
		M1026 Privileged Account Management
		M1027 Password Policies
		M1036 Account Use Policies
Discovery	Network Service Discovery	M1030 Network Segmentation
		M1031 Network Intrusion Prevention
		M1042 Disable or Remove Feature or Program
Execution	Command and Scripting Interpreter: Windows Command Shell	M1038 Execution Prevention
	Software Deployment Tools	M1015 Active Directory Configuration
		M1017 User Training
		M1018 User Account Management
		M1026 Privileged Account Management
		M1027 Password Policies
		M1029 Remote Data Storage
		M1030 Network Segmentation
		M1032 Multi-factor Authentication

Continued

	System Services: Service Execution	M1033 Limit Software Installation
		M1051 Update Software
		M1022 Restrict File and Directory Permissions
		M1026 Privileged Account Management
		M1040 Behavior Prevention on Endpoint
Exfiltration	Exfiltration Over Web Service	M1021 Restrict Web-Based Content
		M1057 Data Loss Prevention
Impact	Data Destruction	M1053 Data Backup
	Data Encrypted for Impact	M1040 Behavior Prevention on Endpoint
		M1053 Data Backup
	Defacement: Internal Defacement	M1053 Data Backup
	Inhibit System Recovery	M1018 User Account Management
		M1028 Operating System Configuration
		M1053 Data Backup
	Service Stop	M1018 User Account Management
		M1022 Restrict File and Directory Permissions
		M1024 Restrict Registry Permissions
		M1030 Network Segmentation
Initial Access	Drive-by Compromise	M1021 Restrict Web-Based Content
		M1048 Application Isolation and Sandboxing
		M1050 Exploit Protection
		M1051 Update Software
	Exploit Public-Facing Application	M1016 Vulnerability Scanning
		M1026 Privileged Account Management
		M1030 Network Segmentation
	External Remote Services	M1030 Network Segmentation
		M1032 Multi-factor Authentication
		M1035 Limit Access to Resource Over Network
		M1042 Disable or Remove Feature or Program
	Phishing	M1017 User Training
		M1021 Restrict Web-Based Content
		M1031 Network Intrusion Prevention
		M1049 Antivirus/Antimalware
		M1054 Software Configuration
	Valid Accounts	M1013 Application Developer Guidance

Continued

		M1015 Active Directory Configuration
		M1017 User Training
		M1018 User Account Management
		M1026 Privileged Account Management
		M1027 Password Policies
		M1036 Account Use Policies
Lateral Movement	Remote Services: Remote Desktop Protocol	M1018 User Account Management
		M1026 Privileged Account Management
		M1028 Operating System Configuration
		M1030 Network Segmentation
		M1032 Multi-factor Authentication
		M1035 Limit Access to Resource Over Network
		M1042 Disable or Remove Feature or Program
		M1047 Audit
	Remote Services: SMB/Windows Admin Shares	M1026 Privileged Account Management
		M1027 Password Policies
		M1035 Limit Access to Resource Over Network
		M1037 Filter Network Traffic
Persistence	External Remote Services	M1030 Network Segmentation
		M1032 Multi-factor Authentication
		M1035 Limit Access to Resource Over Network
		M1042 Disable or Remove Feature or Program
	Valid Accounts	M1013 Application Developer Guidance
		M1015 Active Directory Configuration
		M1017 User Training
		M1018 User Account Management
		M1026 Privileged Account Management
		M1027 Password Policies
		M1036 Account Use Policies
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control	M1026 Privileged Account Management
		M1047 Audit
		M1051 Update Software
		M1052 User Account Control

Continued

	Domain Policy Modification: Group Policy Modification	M1018 User Account Management
		M1026 Privileged Account Management
		M1047 Audit
		M1013 Application Developer Guidance
		M1015 Active Directory Configuration
		M1017 User Training
	Valid Accounts	M1018 User Account Management
		M1026 Privileged Account Management
		M1027 Password Policies
		M1036 Account Use Policies